RED ALERT LABS
IoT Security

CADRE DE CERTIFICATION DE CYBERSECURITE IOT DE L'UE

12 Juin 2018

QUI SUIS-JE?
RA & RAL

RED ALERT LABS
IoT Security

Roland Atoui
Gérant & Fondateur, Red Alert Labs

QUELLES PROBLÉMATIQUES ?

Une nouvelle ère de défi pour la cybersécurité ?

IoT – De quoi parlons-nous ?

Pourquoi aujourd'hui?

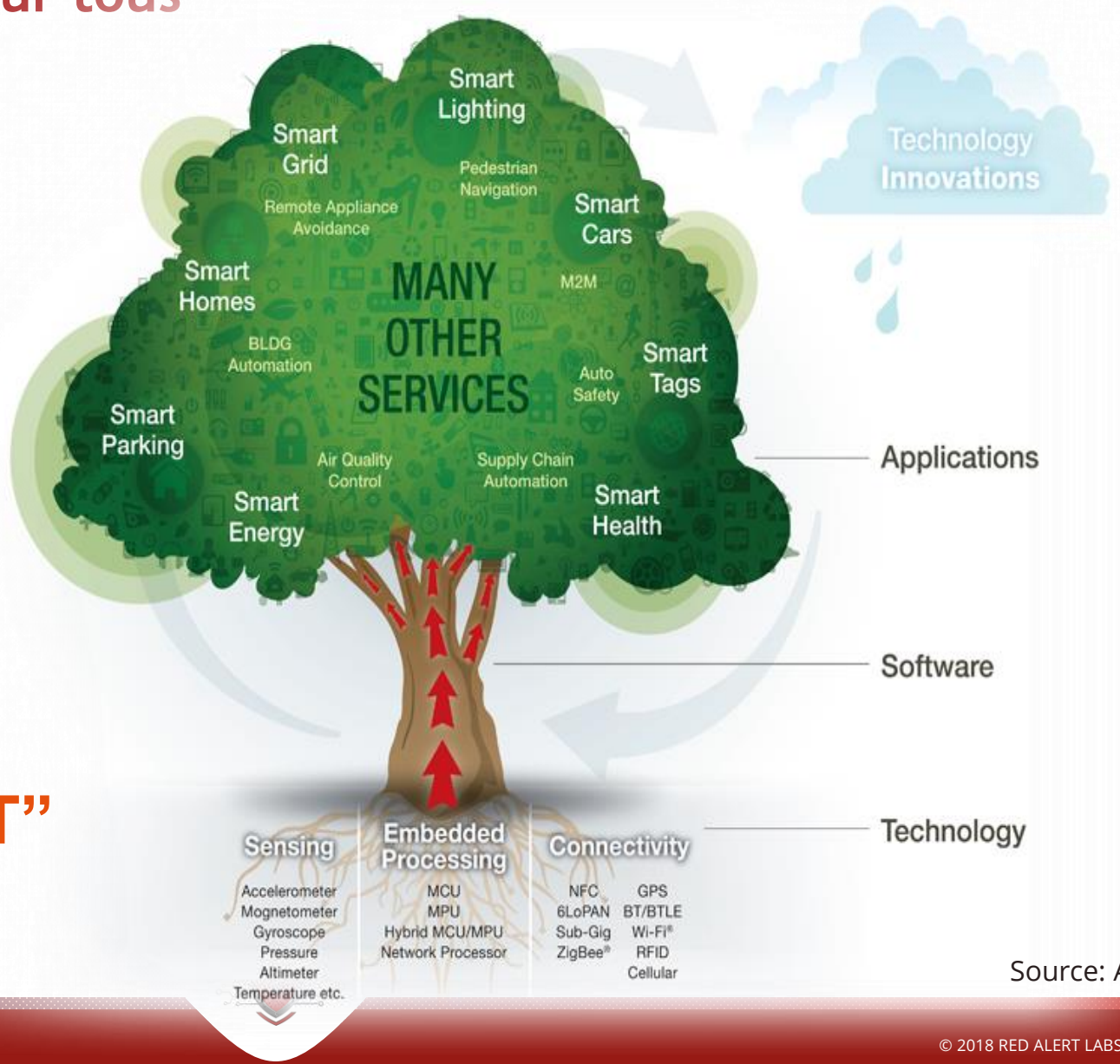
Pourquoi les pratiques et standards existants ne s'appliquent pas à l'IoT ?

Comment pouvons-nous faire confiance aux objets connectés ?

Quelles solutions => Quels objectifs ?

Enfin, qu'est ce que l'EUROPE propose comme solution ?

Internet des Objets
Différents Services, Différentes Technologies
Différentes significations pour tous



Et le mot

“INTELLIGENT”

Est partout !

Source: ARM

Internet des Objets
M2E

L'Internet des Objets (IoT) concerne la Machine aux Entités (M2E):

Machine à Machine :

- Diagnostique automatique pour les voitures : collecte d'informations automatiques à partir du système de gestion de votre voiture et envoyé en temps réel à d'autres voitures, chauffeurs ou centres de service

Machine à Infrastructure :

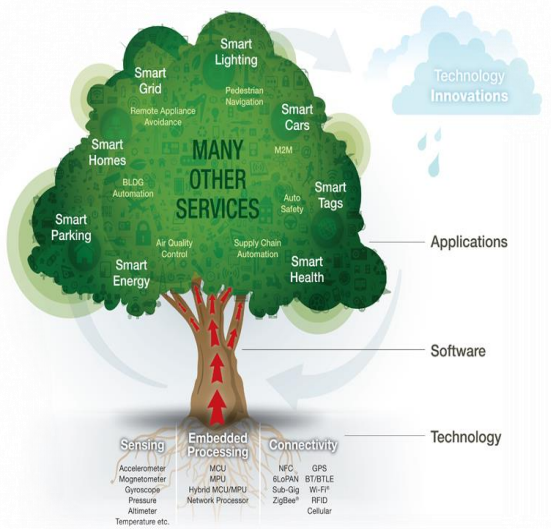
- Surveillance automatique du pont : détection et surveillance de l'intégrité structurelle du pont en cas d'inondation

Machine à Humain :

- Surveillance automatique de la santé des personnes : service de surveillance des implants ou gestion des maladies via des implants électroniques

Machine à Nature/Environnement:

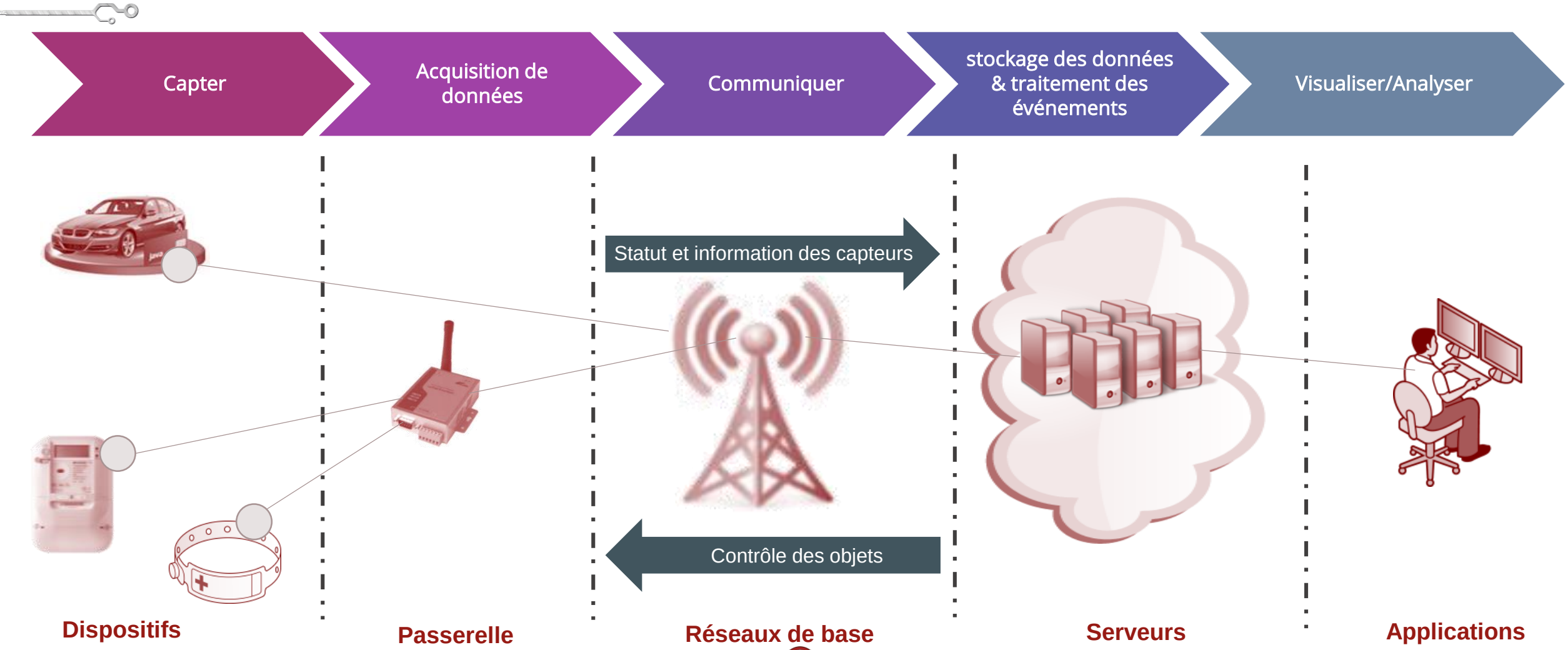
- Détection précoce des tremblements de terre : Répartition de capteurs pour détecter précocement les tremblements à des endroits spécifiques



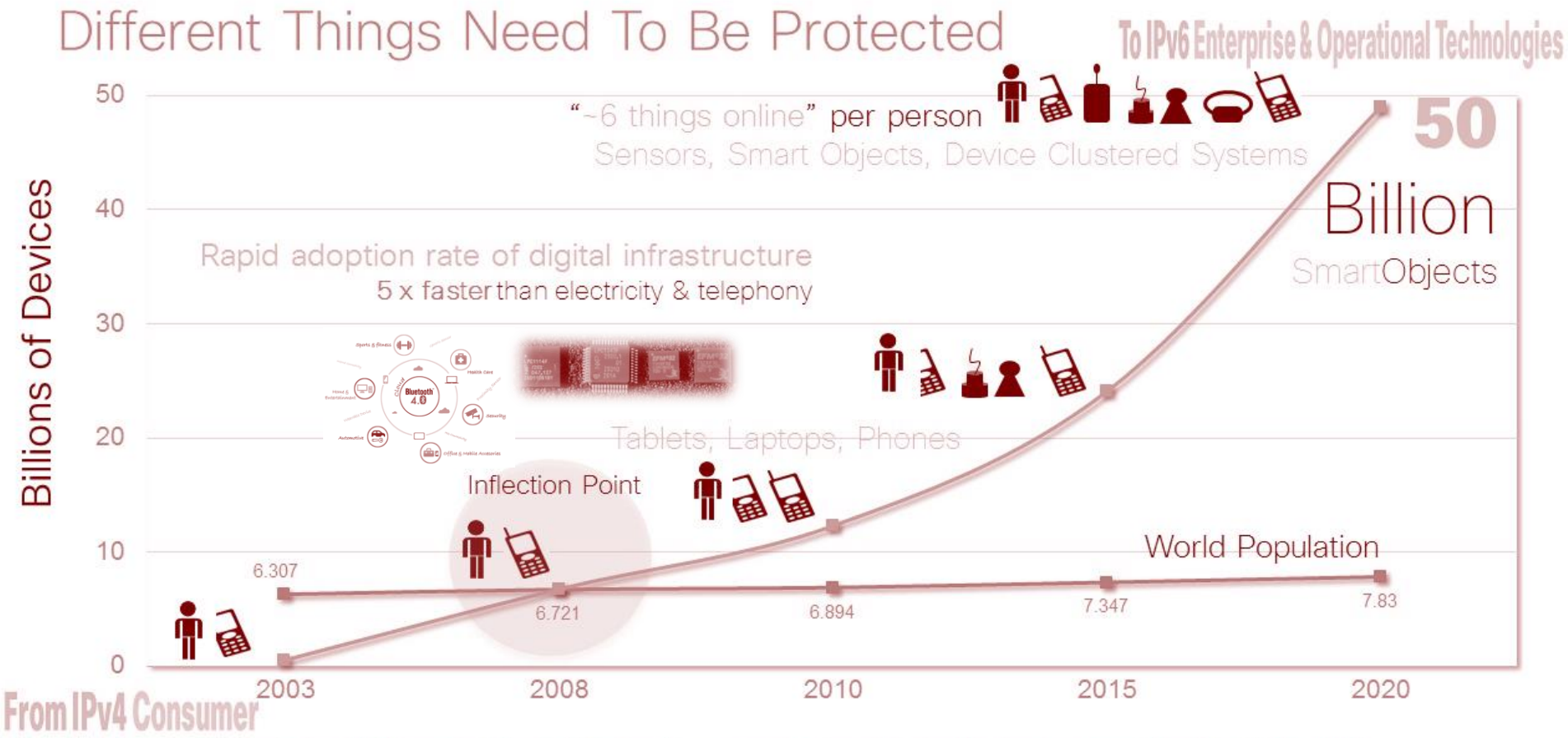
Internet des Objets
PANORAMA

- **Commerce de détail**
  - Spécialité
  - Hospitalité
  - Magasins
- **Transports**
  - Système de transport
  - Véhicules
  - Non-vehiculaire
- **Industriel**
  - Distribution Intelligente
  - Automatisation des ressources
  - Maintenance Prédictive
  - Fabrication intelligente
- **Santé & Sciences de la vie**
  - Santé
  - In vivo/maison
  - Laboratoire de Recherche
- **Consommateurs & Maison**
  - Infrastructure
  - Commodité
  - Divertissement
- **Energie Intelligente**
  - Offre & Demande
  - Huile & Gaz
  - Energie Alternative
- **Bâtiments Intelligents**
  - Commercial
  - Institutionel
  - Industriel
- **TI & Réseaux**
  - Public
  - Entreprise
- **Sûreté & Sécurité Publique**
  - Infrastructure Publique
  - Services d'urgence
  - Surveillance
  - Suivi

Internet des Objets
ARCHITECTURE TYPIQUE



Internet des Objets
EVOLUTION IMPORTANTE ?



Source: Cisco IBSG projections, UN Economic & Social Affairs http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf

L'INTERNET DES OBJETS

AVEC DES RISQUES ÉLEVÉS DE SÉCURITÉ

BEAUCOUP DE BÉNÉFICES mais…


The Economist — World politics | Business & finance | Economics | Science & technology | Culture

Cyber-security

The internet of things (to be hacked)

Hooking up gadgets to the web promises huge benefits. But security must not be an afterthought

Jul 12th 2014 | From the print edition

How the Internet of Things Could Kill You

By Fahmida Y. Rashid JULY 18, 2014 7:30 AM - Source: Tom's Guide US | 5 COMMENTS

Hacking the Fridge: Internet of Things Has Security Vulnerabilities

JESS SCANLON | MORE ARTICLES

JUNE 28, 2014

Philips Hue LED smart lights hacked, home blacked out by security researcher

By Sal Cangeloso on August 15, 2013 at 11:45 am | 7 Comments

Fraude & Abue

Des centaines de millions de télévisions connectées sont potentiellement **vulnérables à la fraude au cliques, les botnets, les vols de données et même les ransomware.**

Les grille-pain sont utilisés comme des botnets pour accéder à votre compte Facebook ou allumer votre webcam

Vie Privée

Des pirates informatiques ont infiltrés le réseau de l'hôpital de l'Université de Californie, Los Angeles, accédant ainsi aux ordinateurs contenant des données sensibles de 4,5 millions de personnes.

Le volume des données augmentent tellement rapidement, que les vendeurs et entreprises manquent de temps pour les protégées adéquatement.

Sureté

Il existe des vulnérabilités potentiellement mortelles dans bon nombre de dispositifs telles que les pompes à insuline et les défibrillateurs implantables.

La US National Nuclear Security Administration a subi 19 cyber-attaques réussi durant la période de 4 ans de 2010 à 2014.

POURQUOI EST-CE SI DIFFICILE DE SÉCURISÉ ?

Menaces de sécurité de l'IoT
3 domaines principaux

GRANDE SURFACE D'ATTAQUE + PLUSIEURS TYPES D'ATTAQUES

Domaine de Service

- Confidentialité
- Disponibilité
- …

Attaque du SERVEUR

Attaque du LOGICIEL

Trust Boundary

Domaine Réseau

- Disponibilité
- Répudiation
- Confidentialité
- Integrité
- Authentification Mutuelle
- ….

Attaque du RÉSEAU

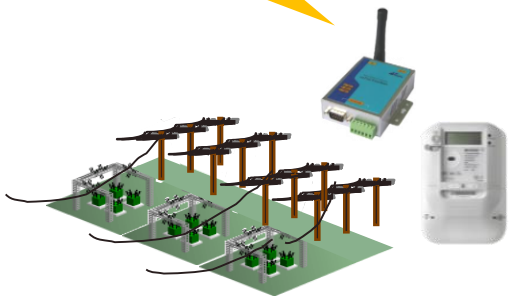
Attaque MITM

Trust Boundary

Domaine des Dispositifs

- Falsification (physique)
- Disponibilité
- Destruction
- Authentification Mutuelle
- …

Attaque PHYSIQUE



Internet des Objets
Pourquoi est-ce si difficile de sécurisé !?

- **Longue vie :** ces systèmes durent jusqu'à 20 ans et leur sécurité devraient en faire autant.
  - Notamment pour les infrastructures critiques
  - Mais doivent s'adapter aux menaces qui évoluent constamment
  - Ceci implique une mise à jour à distance de la sécurité
- **Difficilement accessible :** les dispositifs de l'IoT ne sont pas toujours proche des humains.
  - Ils sont susceptibles d'être exposés aux agresseurs
  - L'utilisateur ne surveille pas l'activité en permanence
- **Contraintes de Ressources (i.e. les piles)**
  - Ressources de traitement limitées
  - Mode veille : les communications ne sont pas toujours en ligne
  - Souvent avec une bande passante limitée
  - Défi de révocation et d'évolutivité

Internet des Objets
Pourquoi est-ce si difficile de sécurisé !?

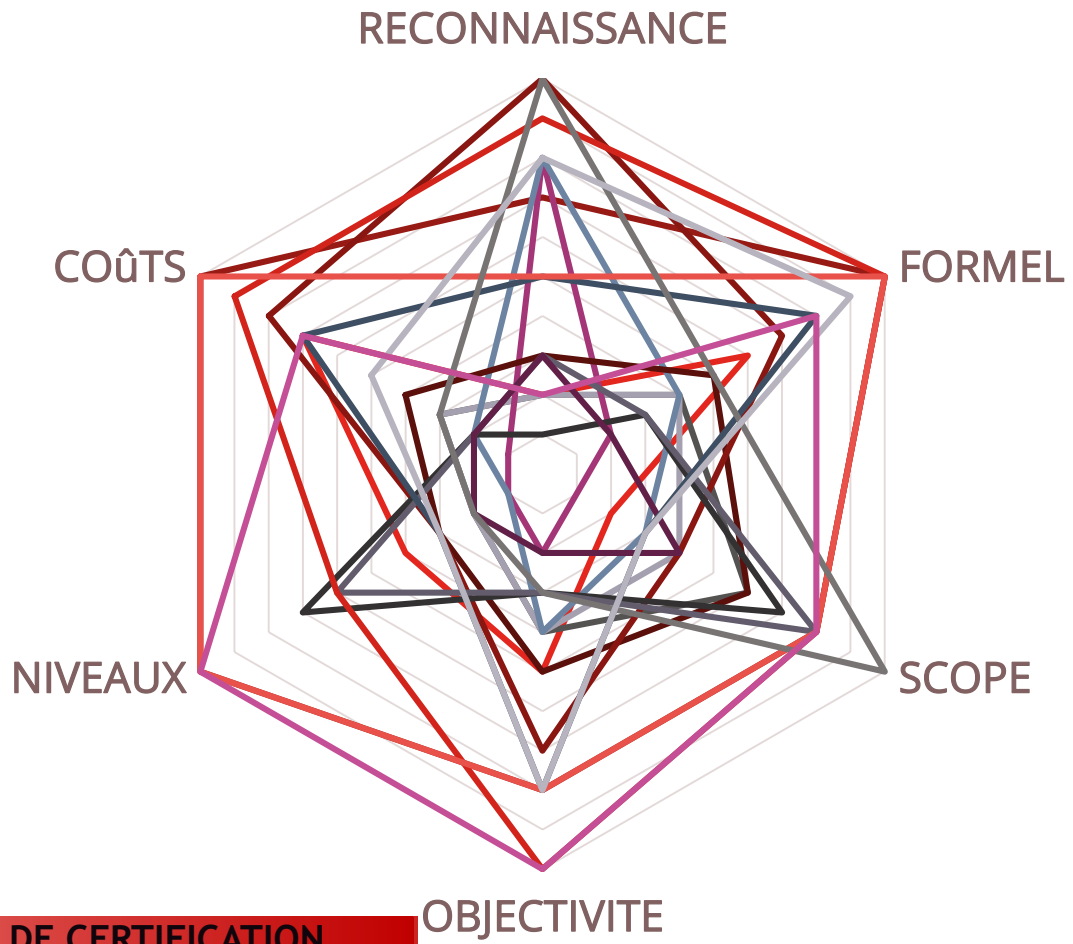
- **Complexe, systèmes distribués**
  - Beaucoup de langage, de système d'exploitation, et de réseaux
  - Matériel informatique spécialisé
- **C'est difficile de développer des applications**
- **Des données précieuses :** personnelles, financières, santé, position, présence

➔ **Pas de temps/d'argent** pour investir dans la sécurité

COMMENT MESURE-T-ON LA SÉCURITÉ ?

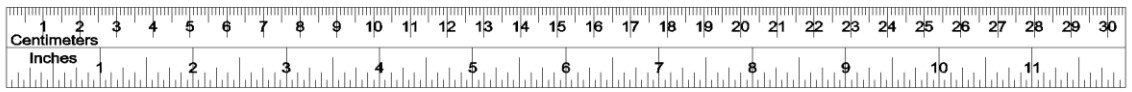
Standards de Certification de Produits

Quelles métriques ?



- CC std
- FIPS 140-2
- CSPN
- CPA
- FIDO L1
- FIDO L2
- UL CAP/2900
- PCI PTS
- UL LSP
- IOTSF
- GSMA IoT
- GP TEE
- CC cPP
- SOGIS
- Pen Testing
- FIDO L3
- ISCCC

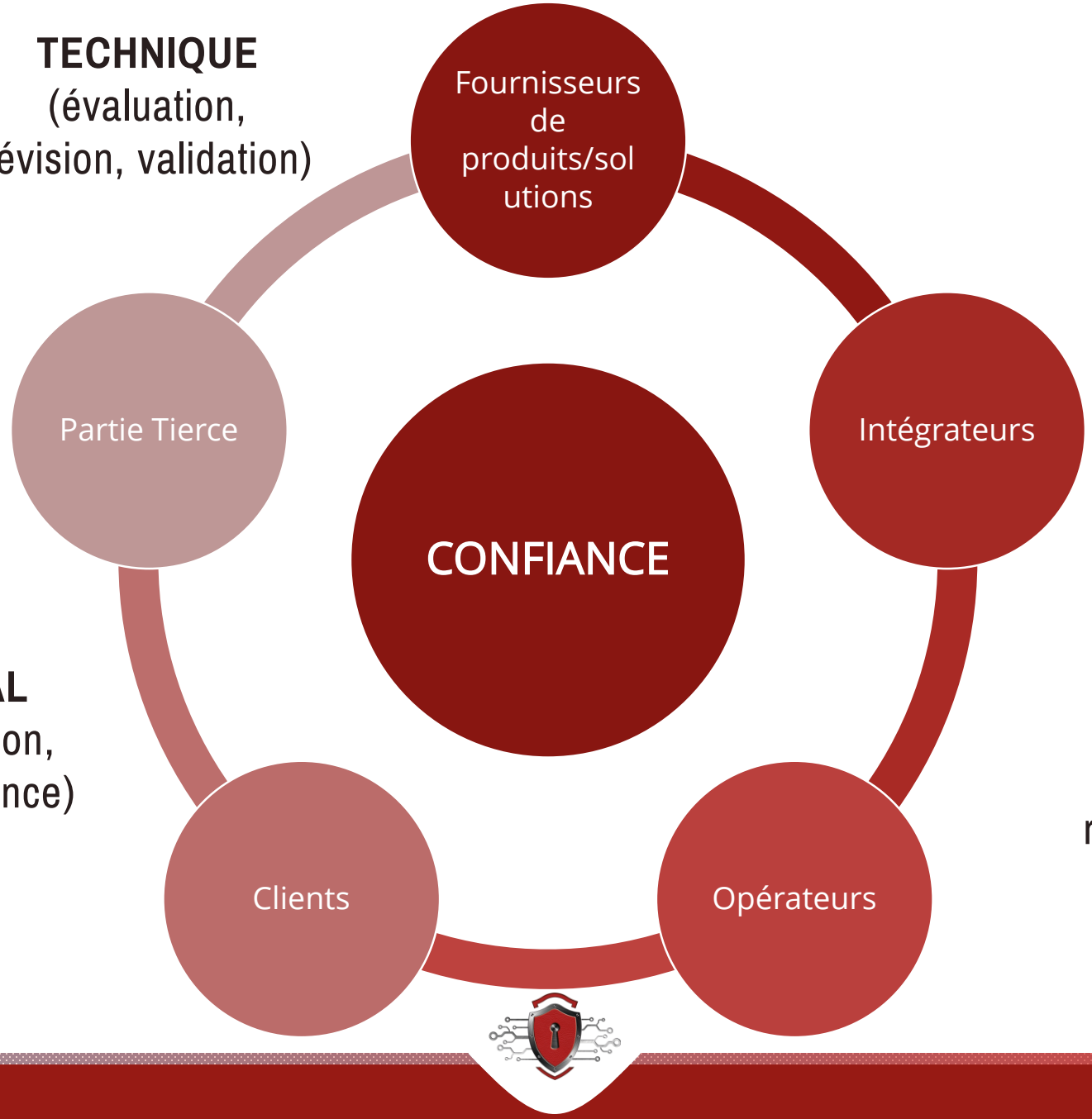
METRIQUES - STANDARDS - SCHEMAS DE CERTIFICATION



À PROPOS DE CONFIANCE

CONFIANCE
DÉFINITION

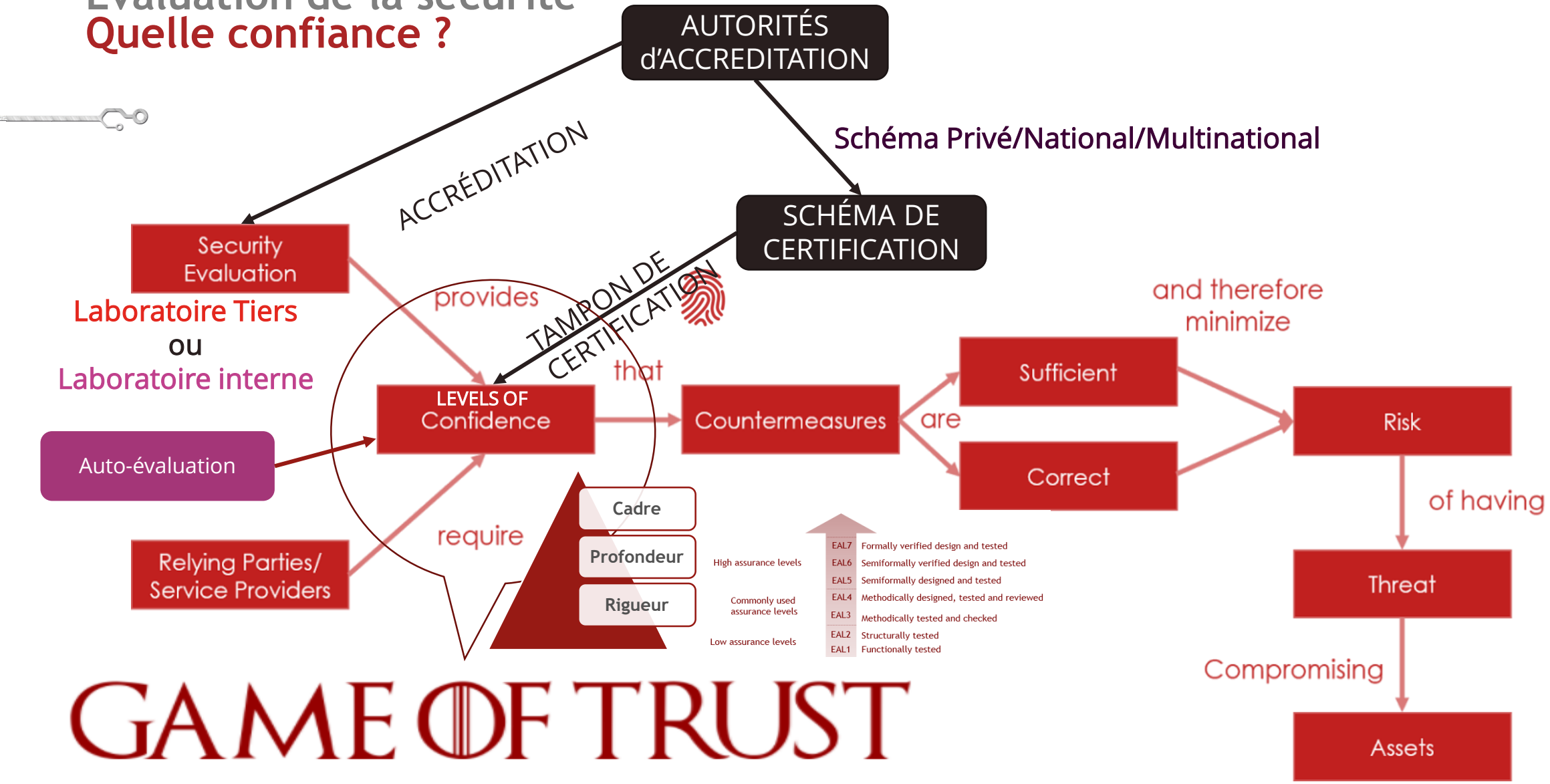
TECHNIQUE
(évaluation, révision, validation)



SOCIAL
(réputation, transparence)

LÉGAL
(régulations, contrats, engagements, responsabilités)

Évaluation de la sécurité
Quelle confiance ?



GAME OF TRUST

QUELLE EST LE PROBLÈME DE CERTIFICATION DE PRODUITS TI AUJOURD'HUI?

Internet des Objets
Problème de la certification des produits

Ça coûte beaucoup d'ARGENT, ça prends un TEMPS considerable et est souvent VALABLE pour une courte durée

- Laboratoire d'Évaluation
- Consultation CC (optionel)
- Développement interne des preuves
- Dépenses pour les visites de sites (optionel)
- Dépenses de voyage (optionel)
- Coût des équipements
- Opportunités manquées
- Schéma de Certification (ANSSI -> FREE, BSI -> 2,5K€ to 12K€)

TOTAL COSTS

➔ Exemple de dépenses pour Laboratoire d'Évaluation:

- **EAL 2**: 80K€ → 150 K€
- **EAL 3**: 120K€ → 200 K€
- **EAL 4+**: 150K€ → 300 K€

Niveau EAL	Temps d'évaluation
EAL 2	4 – 6 mois
EAL 3	6 – 9 mois
EAL 4	7 – 12 mois
>EAL 4	12 – 24 mois

MAIS QUELLE POURRAIT ETRE LA VRAI SOURCE DU PROBLÈME ?

EXPÉRIENCE CONSOMMATEUR/ACHTEUR !

Les fournisseurs sont habitués à différencier les produits basés sur
LES FONCTIONNALITES & LES COÛTS

POURQUOI ?

Parce que les consommateurs ne sont pas habitués à différencier les produits basés sur la SECURITÉ

CARACTÉRISTIQUES ET COÛT vs SÉCURITÉ

➔

Le temps du cycle de vie de fabrication est réduit au MINIMUM

⇒ Pas le temps de concevoir/tester/patcher la securité

DONC POURQUOI NE PAS RÉUTILISER DES TECHNIQUES D'ÉVALUATION DÉJÀ EXISTANTES POUR L'IoT ?

POURQUOI NE PAS RÉUTILISER DES TECHNIQUES D'ÉVALUATION DÉJÀ EXISTANTES ?

- **Coût, temps, validité** - ne peut pas être appliquer aux 50 milliards de produits IoT sur la marché ! Il n'y a pas assez de ressources pour faire ça…
- **Subjectif** - quelle est la crédibilité des laboratoires d'évaluations/pentester/etc. Que signifie sécuriser ? Peut-on comparer plus ou moins des produits sécurisés ?
- Le consommateur ne **ressent/comprend pas la valeur** de la sécurité

POURQUOI NE PAS RÉUTILISER DES TECHNIQUES D'ÉVALUATION DÉJÀ EXISTANTES ?

Aujourd'hui, la sécurité de l'IoT ajoute un gros problème soit le problème COMMERCIAL (TTM, Coût,…)

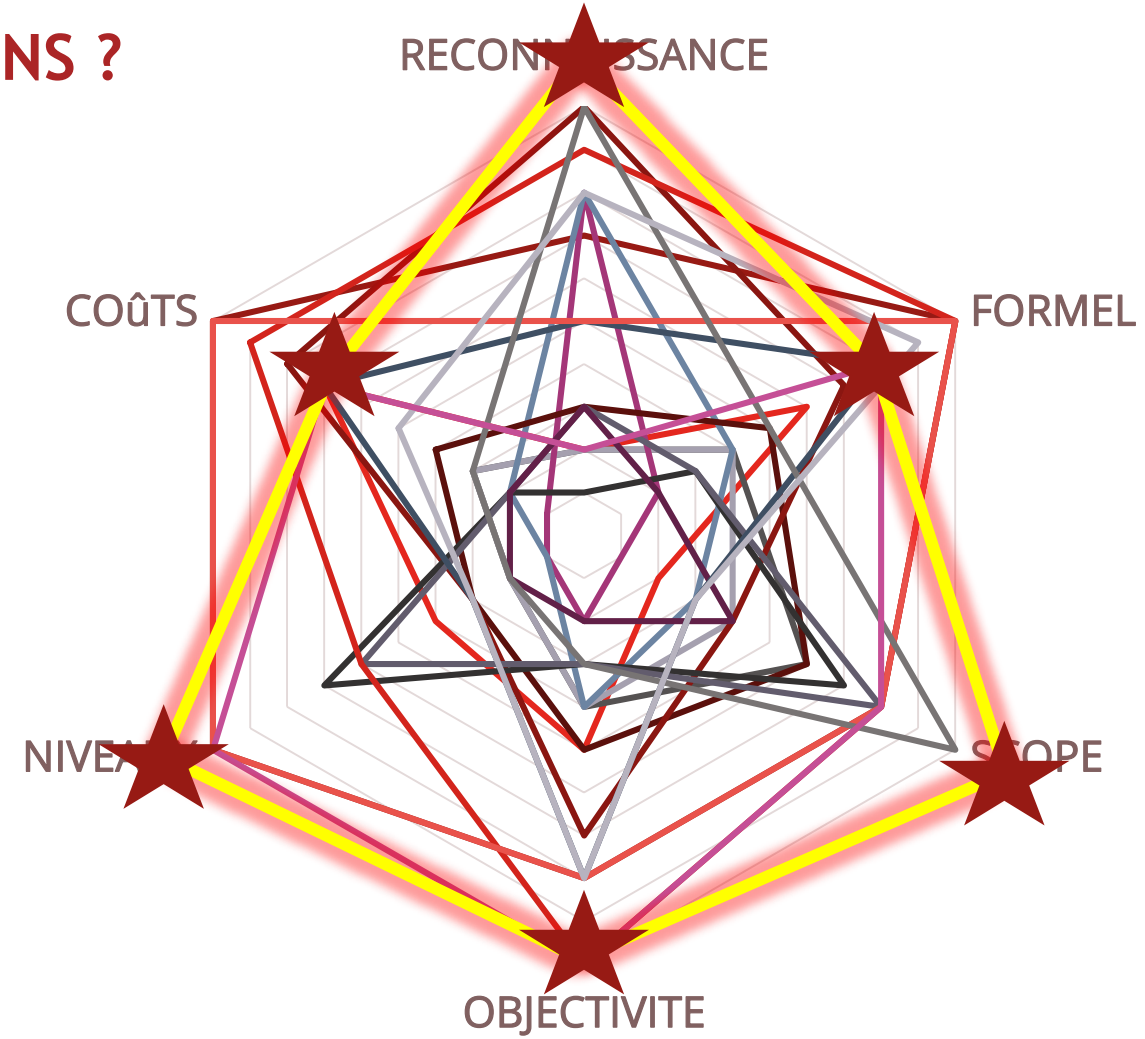
Amplifiant ainsi la complexité des problèmes TECHNIQUES

SOLUTIONS ?

- **Réadapter les cadres de certification de sécurité existants afin de satisfaire les 10 objectifs suivants :**

1. Permettre un cycle de vie de fabrication du produit rapide & agile
2. Réduire les coûts et le temps des évaluations
3. Motiver et sensibiliser le développeur et l'achteur
4. Inclure la formation
5. Reconnaître l'auto-évaluation accréditée (pour un niveau d'assurance de sécurité basique)
6. Fournir des méthodes/métriques simples aux développeurs et évaluateurs
7. Reconnaître les méthodologie d'évaluation et de standards de sécurité existants
8. Considérer l'environnement opérationnel / processus / contexte / domaine complet
9. Autoriser le client et le fournisseur à comparer les différents produits de **MANIÈRE OBJECTIVE (quand il le faut)**
10. Reconnaissance mutuelle

Sécurité de l'IoT
QUELLES SOLUTIONS ?



- CC std
- FIPS 140-2
- CSPN
- CPA
- FIDO L1
- FIDO L2
- UL CAP/2900
- PCI PTS
- UL LSP
- IOTSF
- GSMA IoT
- GP TEE
- CC cPP
- SOGIS
- Pen Testing
- FIDO L3
- ISCCC

Quelle est la réponse de l'UE ?

Certification Sécurité ICT
Situation actuelle & ses problèmes

- Émergence d'initiatives nationales/internationales distinctes sans reconnaissance mutuelle (i.e. France(CSPN), GB (CPA), Allemagne(BSI), Pays-Bas (BSPA), Italie, Suède, Norvège)
- (Internationalement ➔ Common Criteria) où en (Europe ➔ SOG-IS) réussissent jusqu'à présent
  - CCRA (28 EMs)
  - SOG-IS MRA membership (14 EMs)
  - Mais les coûts et la durée peuvent ne pas convenir à tous les besoins du marché
- Difficile de distinguer les produits/services plus ou moins sécurisés
- La coexistence de différents schémas rend la comparaison difficile
- Les utilisateurs finaux s'abstiennent d'acheter des produits certifiés
- Trop d'initiatives pour les standardisations

Standards de sécurité IoT
State of The Art (SOTA)

1. Commission européenne (**CE**) et Alliance pour l'innovation dans l'Internet des objets (**AIOTI**): Rapport sur l'atelier sur la Sécurité et la Confidentialité dans l'Internet des objets (**2017**)
2. Alliance pour l'innovation dans l'Internet des objets (**AIOTI**): Rapport sur l'atelier sur la sécurité et la confidentialité dans le monde hyper-connecté (**2016**)
3. Commission urité et la confidentiali
4. Plateforme
5. Gouverneme rincipes clés de la cybers
6. Départemen
7. Départemen objets (**2016**)
8. Départemen : Gestion de la cybersécu
9. Government Accountability Office des États-Unis: Évaluation des technologies: Internet des objets - Statut et implications d'un monde de plus en plus connecté (**2017**)
10. Institut national des normes et de la technologie (**NIST**): réseaux de «objets» (**2016**)
11. IoT Alliance Australia (**IoTAA**): Ligne directrice sur la sécurité de l'Internet des objets (**2017**)
12. GSM Association (**GSMA**): Document de synthèse sur les directives de sécurité IoT (**2016**)
13. Fondation de sécurité IoT (**IoFST**): Cadre de conformité de sécurité IoT(**2016**)
14. Etc.

➔27 recommandations de sécurité SOTA, Cadres et lignes directrices

➔1.000+ Exigences de sécurité & Principes (350+ Unique)

Certification
4 Options

Option 0:

- Ne rien faire

Option 1:

- Mesures non-législatives – encouragez et soutenir les états membres à rejoindre SOG-IS, soutenir les initiatives de l'industrie, contribuer aux développement des normes de certification.

Option 2:

- Législation Européenne visant à étendre l'accord de SOG-IS pour couvrir tous les états membres. L'ENISA assurerait le rôle de secrétariat.

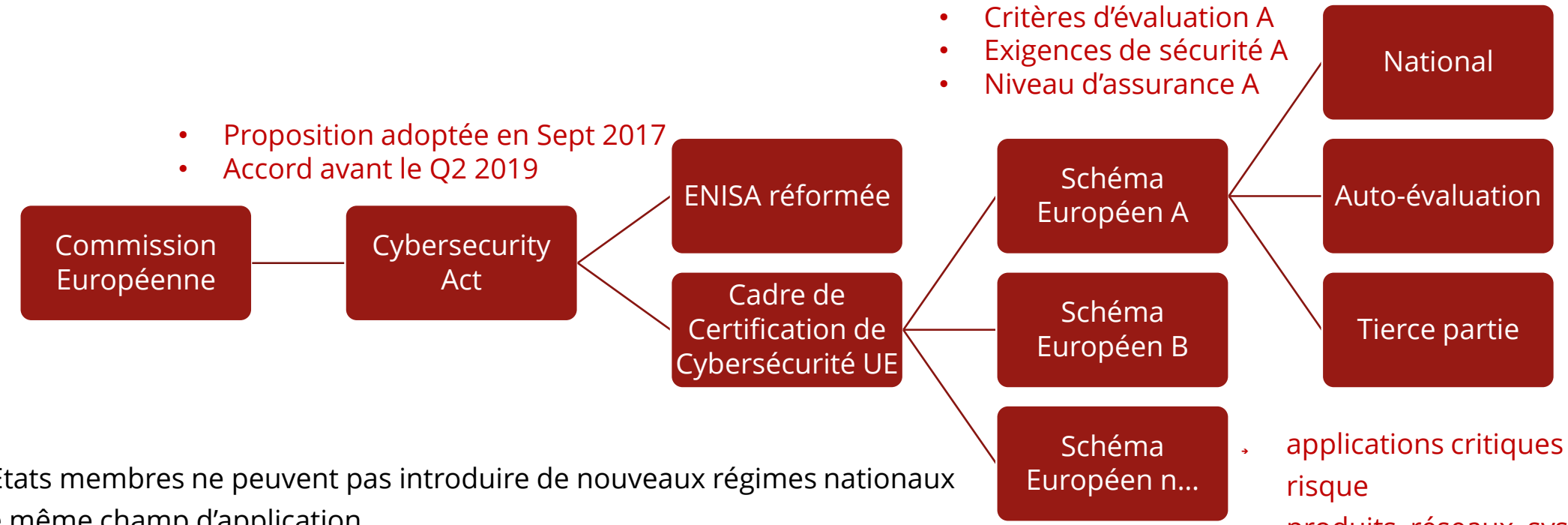
Option 3:

- Législation Européenne visant à créer un cadre de certification de sécurité ICT (incluant un groupe d'experts formé des autorités nationales) en ce basant sur des standards existants. Ce cadre permettra la création de plusieurs schémas de certifications qui seront adoptés par les états membres.

Commission Européenne
Accord sur la Cybersécurité

- Champ d'application A
- Critères d'évaluation A
- Exigences de sécurité A
- Niveau d'assurance A

- Proposition adoptée en Sept 2017
- Accord avant le Q2 2019



➔ Les États membres ne peuvent pas introduire de nouveaux régimes nationaux ayant le même champ d'application

➔ Les régimes nationaux existants couvrant le même produit/service cessent de produire des effets

➔ Les certificats existants des régimes nationaux sont valables jusqu'à la date d'expiration

- applications critiques ou à haut risque
- produits, réseaux, systèmes et services numériques largement déployés
- appareils grand public, numériques et interconnectés à faible coût

CADRE DE CERTIFICATION DE CYBERSECURITE EUROPEEN
Définition

- Un système européen de certification de cybersécurité atteste que les produits et services TIC qui ont été certifiés conformément à ce système satisfont à des exigences spécifiées concernant leur capacité à résister, à un niveau d'assurance donné, à des actions visant à compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services associés qui sont offerts ou accessibles par ces produits, processus, services et systèmes

CADRE DE CERTIFICATION DE CYBERSECURITE EUROPEEN
Objectifs

- Contribuer à la définition d'un cadre institutionnel européen plus cohérent afin de renforcer la résilience commune de l'UE et renforcer la confiance dans le marché unique numérique.
    1. Mettre à disposition un instrument / schéma de l'UE qui soutiendrait les besoins en matière de cybersécurité des États membres, les institutions de l'UE et l'UE dans son ensemble afin de renforcer la résilience en cybersécurité;
    2. Supprimer les obstacles au DSM (Marché Unique Numérique) causés par la coexistence de différents systèmes de certification et l'augmentation de la confiance transfrontalière

Niveaux D'assurance
3 Niveaux

Elémentaire

- un degré limité de fiabilité aux qualités de cybersécurité revendiquées ou prétendues d'un produit ou d'un service TIC.
- **Objectif**: Réduire le risque d'incidents de cybersécurité

Substantiel

- un degré substantiel de fiabilité aux qualités de cybersécurité revendiquées ou prétendues d'un produit ou d'un service TIC.
- **Objectif**: Réduire substantiellement le risque d'incident de cybersécurité

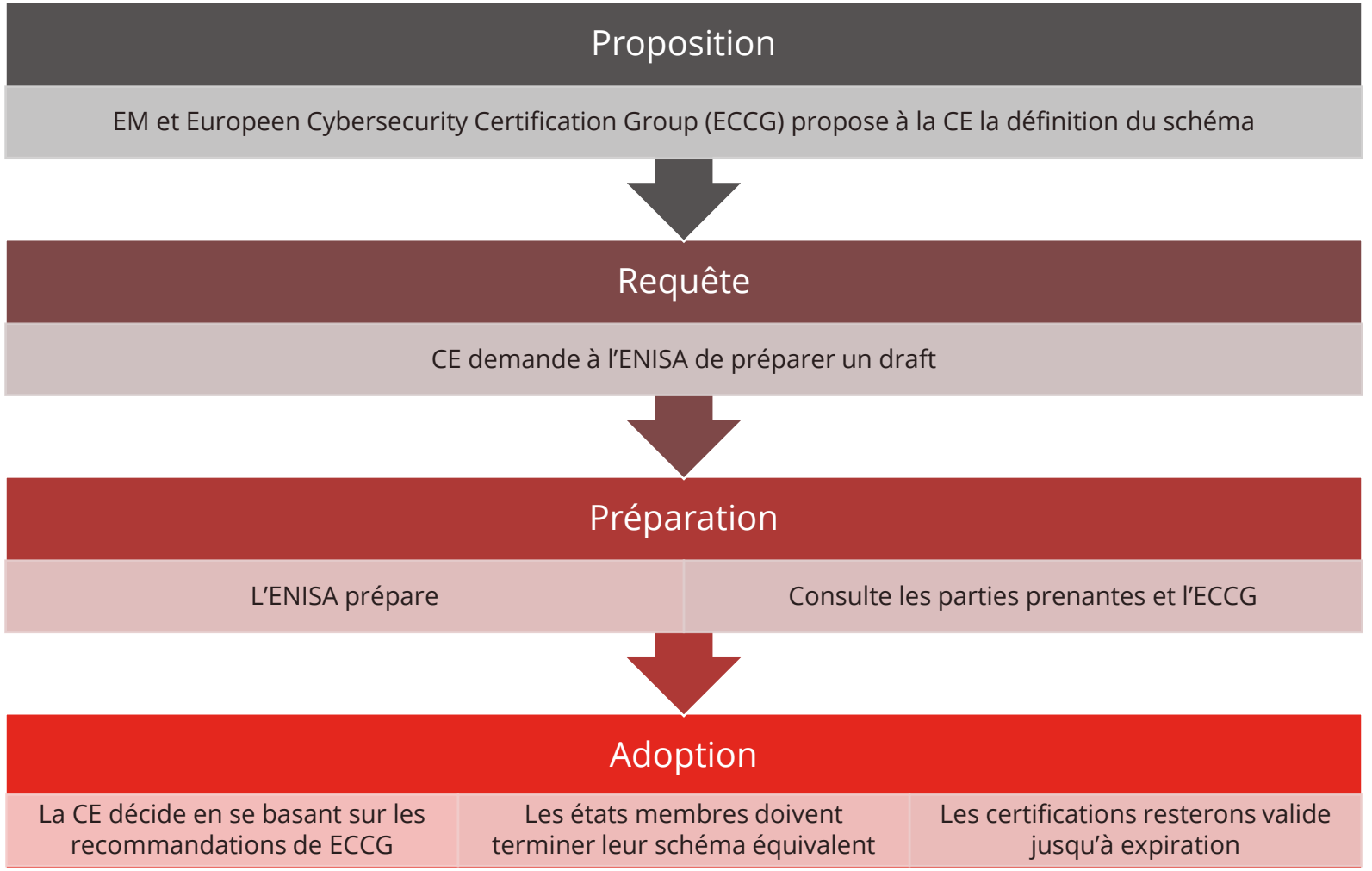
Elevé

- un degré de fiabilité aux qualités de cybersécurité revendiquées ou prétendues d'un produit ou service TIC plus élevé que les certificats ayant le niveau d'assurance substantiel,
- **Objectif**: Prévenir les incidents de cybersécurité

Parties Prenantes
Qui est-ce qui ?

- Autorités nationales de contrôle de la certification
- Organismes d’évaluation de la conformité
- « Le Groupe » européen de certification de cybersécurité
- ENISA
- Schémas Nationaux de Certification

De la Proposition à l'Adoption
Procédure



EU ICT Security Certification Framework
Eléments Clés

3

- Evaluation de conformité aux exigences de sécurité qui seront définies
- 3 x Niveaux d'assurance ?
- Des méthodologies et des Critères d'évaluations spécifiques seront utilisés

5

- La certification est volontaire, sauf indication contraire dans le droit de l'Union.
- Conditions d'utilisation des labels
- Mécanismes de démonstration continue de conformité/Auto-évaluation ?
- Conditions de maintenance et d'extension des certificats

CONTACT

Red Alert Labs

STATION F | 75013, Paris
5 rue Charles de Gaulle | 94140 Alfortville

contact@redalertlabs.com

+33 9 53 55 54 11

www.redalertlabs.com

MERCI POUR VOTRE CONFIANCE

TWITTER @RedAlertLabs

RED ALERT LABS
IoT Security

ANNEX

COMMENT RAL IMPLEMENTE CETTE SOLUTION ?

RAL Sécurité de l'IoT
NOTRE SOLUTION

Sécurité / Très critique Résistant à la fraude	Élevé
Industriel Nécessite une fiabilité robuste et une capacité de sécurité	Modéré
Business Introduire des exigences pour des capacités de sécurité additionnelles, plus de temps pour les analyses de vulnérabilité/Attaques basiques améliorées	Basique amélioré
Commerciale Poussé par la performance et la facilité d'utilisation	Basique

Exigences → Conception → Implémentation → Vérification → Lancement → Réponse

Formation

Analyses de risques IoT

OU

Profil de sécurité standardisé
(type d'appareil IoT sélectionné)

Profil de sécurité IoT

Catalogue des exigences de sécurité du système IoT

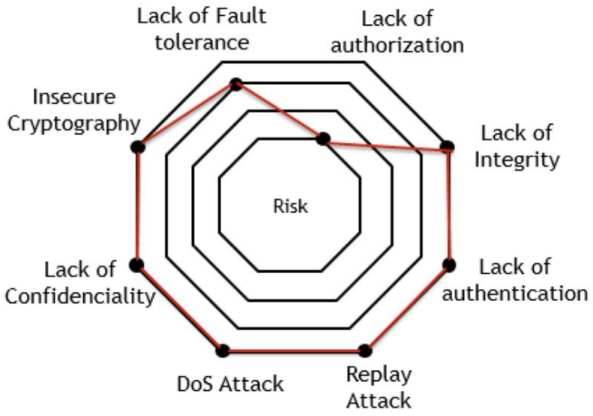
Catalogue des exigences de processus

(de la **vérification** des preuves de certificat à **l'audit**)

Méthodologie d'assurance de sécurité
(Évaluation et certification)
Autoévaluation, évaluation nationale ou évaluation par une tierce partie

(de l'**auto-évaluation** à un **bas niveau de vérification** de la conception)

(d'un **auto-test de sécurité à une analyse de vulnérabilité avancée par un tiers**)



IoT Security Profile (Example)

Security Goal (Sample)	Basic	Enhanced	Advanced
Strong Authentication		X	X
Firmware Integrity			X
Communication Integrity			X
Strong Encryption		X	X
Data Confidentiality		X	X
IP Protection	X	X	X
Data Availability		X	X
Data Privacy	X	X	X
Human Safety			X

IoT System Security Requirements (Example)

Requirements (sample)	Basic	Enhanced	Advanced
Secure Manufacturer-based Identity & Certificate Storage		X	X
Secure Storage (Tamper Resistant)			X
RNG (FIPS or AIS)		X	X
SHA-256 at least		X	X
Secure Onboarding		X	X
Secure Firmware/SW update (digital signature)		X	X
Secure Event Logging		X	X
Limited Data Collection	X	X	X
End User Data Removal	X	X	X
Secure Cloud-Based Management Services		X	X
Active Product Incident Response Team		X	X
Secure Development Lifecycle (SDLC)			X
Data Privacy (Manufacturing)	X	X	X

Assurance Model (Example)

	BASIC SECURITY	ENHANCED SECURITY	ADVANCED SECURITY
CONSUMER ENTREPRISE INDUSTRIAL CRITICAL	• Security Awareness Training • Security Risk Analysis and Best Practices • Compiler Warnings • Set of tests covering Basic Security Requirements	• Secure Coding Guidelines • Design Security Principles and Requirements • Static Code Analysis • Set of tests covering Enhanced Security Requirements • End-of-development Vulnerability Assessment and Penetration Testing • Fuzz Testing	• Ad-hoc security training • Source Code review • Dynamic Security Program Analysis • Set of tests covering Advanced Security Requirements • In-development Agile Vulnerability Assessment and security testing • Final Security Review

RAL Sécurité IoT
NOTRE SOLUTIONS d'AUTO

Catalogue des exigences de sécurité du système IoT

Test des Fonctionalités de Sécurité

Test de vulnérabilité

Test de robustesse (Fuzzing)

Modèles fonctionnels

Les schémas de vulnérabilité

Analyse de risque IoT

OR

Profil de sécurité IoT

Profil de sécurité standardisé (type d'appareil IoT sélectionné)

Modèles de test

Test de Scenarios

Test de Cas

SUT